NHẬN THỨC VỀ TỘI PHẠM CÔNG NGHỆ CAO TRONG THỜI KỲ CÁCH MẠNG CÔNG NGHIỆP 4.0

AWARENESS OF HIGH – TECH CRIME IN THE INDUSTRIAL REVOLUTION 4.0

[1]Ngô Thuỳ Dung, [2]Trần Trung Nguyên
[1] Khoa Lý luận chính trị, [2] Viện Đào tạo Chất lượng cao
Trường Đại học Giao thông vận tải TP.HCM

***Tóm tắt**: Cách mạng công nghiệp lần thứ tư đang diễn ra mạnh mẽ đem lại cho các quốc gia nhiều cơ hội để phát triển kinh tế, văn hóa, xã hội, khoa học công nghệ… Tuy nhiên, cuộc cách mạng này cũng đặt ra nhiều thách thức cho công tác phòng, chống tội phạm đặc biệt là tội phạm công nghệ cao. Nâng cao nhận thức về tội phạm công nghệ cao là nhu cầu của mọi cá nhân, tổ chức để nâng cao hiệu quả đấu tranh phòng, chống nhóm tội phạm này.*

***Từ khóa**: Cách mạng công nghiệp, tội phạm công nghệ cao, tội phạm mạng.*

***Chỉ số phân loại:** 3.5*

***Abstract:** The industrial revolution 4.0 is taking place strongly, giving countries many opportunities for economic, cultural, social, scientific and technological development… However, this revolution also poses many challenges to the prevention and control of crime, especially high-tech crimes. Improve awareness about high-tech crime is the need of all individuals and organizations to improve effectively fighting and preventing of these crimes.*

***Key words:** High-tech crime, industrial revolution 4.0, Cybercrime.*

***Classification number:** 3.5*

1. Giới thiệu

Cuộc cách mạng công nghiệp lần thứ tư (hay còn gọi là: *Cách mạng công nghiệp 4.0)* đang diễn ra với hi vọng đem lại những thay đổi lớn lao trong các lĩnh vực kinh tế, khoa học công nghệ, văn hóa, xã hội. Với Việt Nam cách mạng công nghiệp 4.0 là cơ hội để chúng ta thực hiện việc đón đầu, tranh thủ thành tựu khoa học và công nghệ đẩy nhanh tiến trình công nghiệp hóa, hiện đại hóa đất nước, hội nhập quốc tế và thu hẹp khoảng cách phát triển. Tuy nhiên, cuộc cách mạng này cũng đặt ra nhiều thách thức về an ninh quốc gia, đặc biệt là công tác phòng, chống tội phạm.

C*ách mạng công nghiệp 4.0* là cuộc cách mạng dựa trên nền tảng công nghệ kỹ thuật số, tích hợp tất cả công nghệ thông minh nhất, hiện đại nhất, tạo ra những khả năng mới nhất, tác động sâu sắc đến đời sống kinh tế, chính trị, xã hội, v.v…Nó không chỉ làm đảo lộn mọi mô thức truyền thống văn hóa, tinh thần vốn đã tồn tại trong xã hội, mà còn làm thay đổi bản đồ kinh tế thế giới; làm suy giảm quyền lực của một số quốc gia dựa chủ yếu vào khai thác tài nguyên nhưng lại làm gia tăng sức mạnh của các quốc gia nắm trong tay công nghệ. Cùng với cuộc cách mạng này, một loại hình tội phạm mới đã ra đời và ngày càng phát triển. Đó là tội phạm công nghệ cao, loại tội phạm này đã và đang đe dọa tới an ninh của các quốc gia trên thế giới vì khoa học và công nghệ phát triển quá nhanh, trong khi cơ sở hạ tầng kỹ thuật chưa đáp ứng, trình độ công nghệ thông tin còn nhiều hạn chế. Tìm hiểu về tội phạm công nghệ cao là nhu cầu thiết yếu để nâng cao hiệu quả công tác đấu tranh, phòng, chống tội phạm của cơ quan nhà nước cũng là chìa khóa để người dân có thể tự bảo vệ mình. Trong bài viết này tác giả sẽ trình bày những vấn đề cơ bản để người đọc có thể nhận diện nhóm tội phạm này thông qua việc phân tích định nghĩa, đặc điểm của tội phạm công nghệ cao trong Luật Hình sự Việt Nam, đồng thời đưa ra những giải pháp để phòng, chống tội phạm công nghệ cao.

2. Định nghĩa tội phạm công nghệ cao

Thuật ngữ "tội phạm công nghệ cao" được đề cập trong hệ thống pháp luật nhiều nước trên thế giới với nhiều tên gọi khác nhau như: Tội phạm công nghệ cao (high-tech crime); tội phạm máy tính (computer crime): Tội phạm liên quan đến máy tính (computer-related crime); tội phạm mạng (cybercrime)...

Từ điển luật học Black's Law định nghĩa, tội phạm máy tính là: *"Tội phạm đòi hỏi về kiến thức công nghệ máy tính chẳng hạn như phá hoại hoặc ăn cắp dữ liệu máy tính hay sử dụng máy tính để thực hiện một số tội phạm khác"* [1].

Theo từ điển Bách khoa Công an nhân dân: *"Tội phạm công nghệ cao là loại tội phạm có sử dụng những thành tựu mới của khoa học – kỹ thuật và công nghệ hiện đại làm công cụ, phương tiện thực hiện hành vi phạm tội một cách cố ý hay vô ý gây nguy hiểm cho xã hội"* [2].

Trong pháp luật Việt Nam, tội phạm công nghệ cao được đề cập trực tiếp trong Nghị định số: 25/2014/NĐ-CP của Chính phủ với tên gọi: tội phạm sử dụng công nghệ cao. Theo khoản 1, Điều 3: *"Tội phạm có sử dụng công nghệ cao là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự có sử dụng công nghệ cao"* [4].

Trong đó cụm từ công nghệ cao được hiểu là: Công nghệ có hàm lượng cao về nghiên cứu khoa học và phát triển công nghệ; được tích hợp từ thành tựu khoa học và công nghệ hiện đại; tạo ra sản phẩm có chất lượng, tính năng vượt trội, giá trị gia tăng cao, thân thiện với môi trường; có vai trò quan trọng đối với việc hình thành ngành sản xuất, dịch vụ mới hoặc hiện đại hóa ngành sản xuất, dịch vụ hiện có [3].

Trong Luật An ninh mạng 2018, tội phạm công nghệ cao được đề cập với tên gọi khác là tội phạm mạng, theo đó: *"Tội phạm mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự"* [7].

Từ các định nghĩa và khái niệm trên, ta có thể thấy điểm chung trong nội hàm của các khái niệm này đều chỉ các hành vi phạm tội liên quan đến việc sử dụng máy tính, thiết bị số, khai thác mạng máy tính, mạng viễn thông để gây tổn hại cho lợi ích của các tổ chức, cá nhân và toàn xã hội. Ngoài ra tội phạm công nghệ cao còn tác động đến thông tin và dữ liệu điện tử được lưu trữ, truyền phát trong mạng viễn thông và thiết bị số.

Do vậy theo tác giả: *"Tội phạm công nghệ cao là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự được thực hiện một cách cố ý, sử dụng tri thức, kỹ năng, công cụ, phương tiện kỹ thuật số tác động trái pháp luật đến thông tin, dữ liệu, tín hiệu được lưu trữ, xử lý, truyền tải trong hệ thống mạng máy tính, mạng viễn thông, thiết bị số, xâm phạm đến trật tự an toàn thông tin, gây tổn hại lợi ích của Nhà nước, quyền và các lợi ích hợp pháp của các tổ chức, cá nhân".*

3. Đặc điểm

Tội phạm công nghệ cao là hành vi vi phạm pháp luật có tính chất đặc biệt do vậy để nhận diện tội phạm này chúng ta phải dựa vào các đặc điểm cơ bản sau:

Thứ nhất: *Tội phạm công nghệ cao phải là những hành vi vi phạm được quy định trong Luật Hình sự.* Hành vi vi phạm pháp luật có sử dụng công nghệ cao gồm nhiều loại với nhiều mức độ tuy nhiên chỉ những hành vi được quy định trọng Bộ luật Hình sự mới được coi là tội phạm.

Những hành vi vi phạm tuy có sử dụng công nghệ cao xâm phạm đến trật tự an toàn thông tin, gây tổn hại lợi ích của Nhà nước, quyền và các lợi ích hợp pháp của các tổ chức, cá nhân nếu không được quy định trong Bộ luật Hình sự thì không phải là tội phạm. Những hành vi này sẽ bị xử lý về mặt hành chính, dân sự theo những quy định của pháp luật.

Thứ hai: *Tội phạm công nghệ cao bắt buộc phải sử dụng công cụ, phượng tiện có yếu tố công nghệ cao.* Sự khác biệt giữa tội phạm truyền thống có sử dụng công nghệ cao và tội phạm công nghệ cao chính là công cụ, phương tiện phạm tội. Tội phạm công nghệ cao bắt buộc phải sử dụng máy móc thiết bị, công nghệ kỹ thuật số thì mới thực hiện được hành vi phạm tội, còn tội phạm truyền thống không có những công cụ, phương tiện này thì hành vi phạm tội vẫn có thể được thực hiện: tội gián điệp (Điều 110), tội đánh bạc (Điều 321), tội truyền hóa văn hóa phẩm đồi trụy (Điều 326) [5] …

Sự khác biệt về công cụ, phương tiện phạm tội đã khiến cho tội phạm công nghệ cao

có thể thực hiện những hành vi mà tội phạm truyền thống không thể làm được như: Chiếm quyền kiểm soát của một hệ thống điều khiển vận hành bằng công nghệ thông tin như nhà ga, sân bay, mạng lưới giao thông… đánh cắp tiền từ tài khoản ngân hàng, đánh cắp dữ liệu …từ điện thoại, máy tính của bất kỳ ai, ở bất kỳ khu vực hay nơi nào trên thế giới miễn là thiết bị đó có kết nối Internet.

Như vậy với sự hỗ trợ của các công cụ, phương tiện công nghệ cao, tội phạm này có thể tác động đến nhiều đối tượng, ở một phạm vi rộng lớn.

Thứ ba: *Chủ thể tội phạm có trình độ, hiểu biết, kỹ năng về công nghệ thông tin.* Những tội phạm thông thường, người thực hiện hành vi không có yêu cầu về trình độ, kỹ năng công nghệ thông tin.

Nhưng với nhóm tội phạm công nghệ cao người thực hiện hành vi phải có hiểu biết nhất định về công nghệ thậm trí trình độ công nghệ thông tin của họ còn cao hơn những người bình thường.

Tuy nhiên, người thực hiện hành vi này chỉ phải chịu trách nhiệm hình sự nếu có đủ năng lực trách nhiệm hình sự theo quy định của Luật Hình sự. Cụ thể: Đủ 16 tuổi trở lên, có khả năng nhận thức và điều khiển hành vi bình thường.

Thứ tư**:** *Khách thể tội phạm công nghệ cao là trật tự an toàn thông tin*. Tội phạm công nghệ cao xâm phạm đến trật tự an toàn thông tin được Nhà nước bảo vệ, gây tổn hại cho lợi ích của Nhà nước, quyền và các lợi ích hợp pháp của các tổ chức cá nhân.

Trật tự an toàn thông tin bao gồm các quy tắc đảm bảo an toàn thông tin và những quy tắc liên quan đến trật tự pháp luật trong khai thác, sử dụng thông tin do Nhà nước đặt ra [8].

Thứ năm: *Lỗi của chủ thể là lỗi cố ý.* Người phạm tội nhận thức rõ hành vi của mình là nguy hiểm, là trái quy định của pháp luật, có thể gây ra thiệt hại cho người khác hoặc xã hội nhưng vẫn thực hiện, mong muốn hoặc để mặc cho những hậu quả này xảy ra.

Quan điểm này của tác giả có sự khác biệt so với khái niệm về tội phạm sử dụng công nghệ cao được đưa ra trong Từ điển Công an nhân dân cho rằng tội phạm này có thể thực hiện với lỗi cố ý hoặc vô ý.

4. Tội phạm công nghệ cao trong Luật Hình sự Việt Nam

Tội phạm công nghệ cao không phải là một tội danh độc lập được quy định trong Bộ luật Hình sự mà là tổ hợp của những tội phạm sử dụng tri thức, phương tiện công nghệ cao để xâm phạm các quan hệ xã hội được Luật Hình sự bảo vệ.

Tội phạm công nghệ cao sẽ bị xử lý hình sự theo quy định tại mục 2 - Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, chương 21 của Bộ luật Hình sự năm 2015 gồm 10 tội danh: Tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật (Điều 285); Tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 286); Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (Điều 287); Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 288); Tội xâm phạm trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác (Điều 289); Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điển tử thực hiện hành vi chiếm đoạt tài sản (Điều 290); Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng (Điều 291); Tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông (Điều 292); Tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh (Điều 293); Tội cố ý gây nhiễu có hại (Điều 294) [5].

Tuy nhiên xuất phát từ tình hình thực tế khi sửa đổi, bổ sung năm 2017, Bộ luật Hình sự đã bỏ tội danh được quy định tại Điều 292: Tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông [6]. Như vậy, hiện nay còn chín tội phạm công nghệ cao được quy định trong Bộ luật Hình sự.

5. Giải pháp phòng chống tội phạm công nghệ cao

Một là, mỗi tổ chức, cá nhân cần tăng cường bảo vệ mật khẩu, khóa mật khẩu, cơ sở dữ liệu, thông tin cá nhân, thông tin tài khoản và hệ thống thiết bị công nghệ cao của mình bằng các biện pháp cụ thể như thường xuyên thay đổi mật khẩu, thiết lập bảo mật nhiều bước, cài đặt các phần mềm quét virút…; cẩn trọng với những thao tác trên máy tính, điện thoại không click vào những đường dẫn không rõ nguồn gốc, nội dung được gửi tới thiết bị; đọc kỹ những điều khoản khi cài đặt các ứng dụng trên máy tính, điện thoại; không cung cấp thông tin cá nhân một cách tùy tiện.

Hai là, tăng cường phối hợp trong công tác quản lý nhà nước, gắn công tác đấu tranh phòng, chống loại tội phạm này với các lĩnh vực phát triển khoa học, kỹ thuật, công nghệ của đất nước.

Đẩy mạnh công tác tuyên truyền, giáo dục phòng chống tội phạm công nghệ cao qua đó nâng cao ý thức, trách nhiệm phòng ngừa những nguy cơ xâm hại của tội phạm sử dụng công nghệ cao.

Ba là, *x*ây dựng, phát triển lực lượng cảnh sát phòng, chống tội phạm công nghệ cao có số lượng, trình độ ngang tầm nhiệm vụ trong tình hình mới.

Chú trọng tuyển chọn, thu hút chuyên gia giỏi về công nghệ thông tin, viễn thông mới có thể đấu tranh phòng, chống tội phạm công nghệ cao; đồng thời thường xuyên đào tạo, bồi dưỡng, tập huấn nhằm nâng cao trình độ nghiệp vụ, pháp luật, ngoại ngữ, kiến thức và kỹ năng sử dụng phương tiện, thiết bị công nghệ cao cho đội ngũ cán bộ chuyên trách, cử người đủ tiêu chuẩn về phẩm chất chính trị, đạo đức, trình độ đi học tập, bồi dưỡng tại các cơ sở đào tạo uy tín trong và ngoài nước.

Bốn là, nghiên cứu và phổ biến phương thức, thủ đoạn và nguy cơ, tác hại của tội phạm công nghệ cao. Trang bị cho các tổ chức và cá nhân kiến thức, kỹ năng tự phòng, chống tội phạm công nghệ cao; kỹ năng ứng phó khi bị tấn công, xâm nhập trái phép vào hệ thống thông tin, cơ sở dữ liệu.

Năm là, tăng cường hợp tác quốc tế trong lĩnh vực đấu tranh phòng, chống tội phạm sử dụng công nghệ cao. Tập trung trao đổi thông tin tội phạm, ký kết, gia nhập điều ước quốc tế về dẫn độ, xử lý đối với tội phạm sử dụng công nghệ cao; phối hợp thực hiện các hoạt động tương trợ tư pháp trong phòng ngừa, đấu tranh chống tội phạm công nghệ cao.

Thu thập, nghiên cứu, trao đổi thông tin, kinh nghiệm phòng, chống tội phạm công nghệ cao với các nước trên thế giới. Phối hợp với các quốc gia đào tạo, bồi dưỡng, huấn luyện nghiệp vụ về phòng, chống tội phạm công nghệ cao cho lực lượng cán bộ chuyên trách.

6. Kết luận

Cách mạng công nghiệp 4.0 đã và đang tác động mạnh mẽ đến mọi khía cạnh của cuộc sống. Những tác động tích cực mà cuộc cách mạng này mang lại cho nền kinh tế, văn hóa, xã hội của Việt Nam là điều không thể phủ nhận. Tuy nhiên, thách thức đặt ra là tội phạm công nghệ cao ngày càng gia tăng với phương thức, thủ đoạn ngày càng tinh vi.

Do vậy, Nhà nước cần nhanh chóng hoàn thiện hệ thống pháp luật, tăng cường các thiết chế để giám sát và xử lý tội phạm công nghệ cao. Các tổ chức, cá nhân cần nâng cao ý thức trách nhiệm và ý thức cảnh giác với nhóm tội phạm này đồng thời áp dụng nhiều biện pháp kỹ thuật để đảm bảo an toàn thông tin, dữ liệu cho các thiết bị của mình❑

Tài liệu tham khảo

[1] Henry Campbell Black, *Black's Law Dictionary*, Nxb West Publishing Co, 1968;

[2] Từ điển bách khoa Công an nhân dân (2005), NXB Từ điển Bách khoa, Hà Nội.

[3] Luật số: 21/2008/QH12, *Luật công nghệ cao* được Quốc hội nước Cộng hoà xã hội chủ nghĩa Việt Nam khoá XII, kỳ họp thứ 4 thông qua ngày 13 tháng 11 năm 2008;

[4] Nghị định số 25/2014/NĐ-CP của Chính phủ: *Quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao* được ban hành ngày 7 tháng 4 năm 2014;

[5] Luật số 100/2015/QH13, *Bộ luật Hình sự* được Quốc hội nước Cộng hoà xã hội chủ nghĩa Việt Nam thông qua ngày 27/11/2015;

[6] Luật số: 12/2017/QH14, *Luật sửa đổi, bổ sung một số điều của Bộ luật Hình sự số 100/2015/QH13* được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam thông qua ngày 20 tháng 6 năm 2017;

[7] Luật số 24/2018/QH14, *Luật an ninh mạng* được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam thông qua ngày 12 tháng 6 năm 2018;

[8] Hoàng Việt Quỳnh, *Một số trao đổi về tội phạm sử dụng công nghệ cao theo quy định của pháp luật việt nam*, Tạp chí Khoa học Giáo dục Cảnh sát nhân dân số 79 (tháng 8/2016).

Ngày nhận bài: 17/4/2019
Ngày chuyển phản biện: 20/4/2019
Ngày hoàn thành sửa bài: 10/5/2019
Ngày chấp nhận đăng: 17/5/2019